IN THE CLAIMS

Please amend the claims as follows:

1.(Currently Amended)   A digital interface device for facilitating key encryption of a digital signal which is communicated from a computer system to an associated peripheral device, where the associated peripheral device decrypts the communicated digital signal for use, the interface device comprising:

a digital output;

digital output formatting circuitry associated with said output;

a non-volatile RAM for containing a BIOS for controlling digital output formatting having a specific write-protectable area allocated for storing an encryption key flag at a flag address and encryption key data; and

said specific write-protectable area being rendered read-only only when a predetermined flag value is stored at said flag address whereby encryption key data may be stored in said specific area of said non-volatile RAM in connection with storing said predetermined flag value at said flag address such that stored encryption key data cannot be altered by a subsequent write operation to said non-volatile RAM.

2. (Currently Amended) A digital interface device according to claim 1 configured to receive ~~either~~ a first predetermined flag value at said flag address in association with ~~key~~ encryption <u>key</u> data in said specific write-protectable area which first flag value indicates encryption enablement.

3. (Currently Amended) A digital interface device according to claim 1 configured to receive either a first predetermined flag value at said flag address in association with ~~key~~ encryption <u>key</u> data in said specific write-protectable area which first flag value indicates encryption enablement or a second predetermined flag value at said flag address which second flag value indicates encryption disablement in which case the digital interface device is permanently disabled from using the key encryption.

4. (Original) A digital interface device according to claim 1 configured to receive as said predetermined value any value other than a specific value which specific value enables writing into said write-protectable area.

5. (Previously Presented) A digital interface device according to claim 1 wherein said key flag is a combination of one or more values stored at the one or more flag addresses within said write-protectable area.

6. (Original) A digital interface device according to claim 1 wherein the associated peripheral device is a digital display and said digital output is an output port for a digital video signal.

7. (Original) A digital interface device according to claim 6 which is configured as a digital video interface card.

8. (Original) A digital interface device according to claim 1 wherein said specific write-protectable area is at least 512k bytes and located at an address range higher than an address range reserved for a BIOS.

9. (Previously Presented) A method for producing digital interface devices comprising:

providing a digital interface device having a digital output, digital output formatting circuitry associated with said output, and a non-volatile RAM for containing a BIOS for controlling digital output formatting;

allocating a specific addressable area on said non-volatile RAM for storing an encryption key flag and encryption key data; and

rendering said specific area read-only only when a predetermined key flag value is written in said specific addressable area at a key flag address.

10. (Currently Amended) A method according to claim 9 further comprising:

writing a first predetermined flag value at said key flag address along with ~~key~~ encryption <u>key</u> data in said specific area to enable key encryption.

11. (Currently Amended) A method according to claim 9 further comprising:

writing a first predetermined flag value at said key flag address along with ~~key~~ encryption <u>key</u> data in said specific area to enable key encryption; or

writing a second predetermined flag value at said key flag address to permanently disable key encryption using said specific area.

12. (Original) A method according to claim 9 further comprising storing a specific value in said key flag address at the time the specific addressable area is allocated wherein said predetermined key value is any value other than said specific value.

13. (Currently Amended) A digital video interface device for facilitating key encryption of a digital video signal which is communicated from a computer system to an associated peripheral device, where the associated peripheral device decrypts the communicated digital video signal for use, the interface device comprising:

a digital video output;

digital video output formatting circuitry associated with said output;

a non-volatile RAM for containing a BIOS for controlling digital video output formatting having a specific write-protectable area allocated for storing an encryption key flag at a flag address and encryption key data; and

said specific write-protectable area being rendered read-only only when a predetermined flag value is stored at said flag address whereby encryption key data may be stored in said specific area of said non-volatile RAM in connection with storing said predetermined flag value at said flag address such that stored encryption key data cannot be altered by a subsequent write operation to said non-volatile RAM.

14. (Currently Amended) A digital video interface device according to claim 13 configured to receive a first predetermined flag value at said flag

address in association with ~~key~~ encryption <u>key</u> data in said specific write-protectable area which first flag value indicates encryption enablement.

15. (Currently Amended) A digital video interface device according to claim 13 configured to receive either a first predetermined flag value at said flag address in association with ~~key~~ encryption <u>key</u> data in said specific write-protectable area which first flag value indicates encryption enablement or a second predetermined flag value at said flag address which second flag value indicates encryption disablement in which case the digital interface device is permanently disabled from using the key encryption.

16. (Currently Amended) A digital video interface device for facilitating key encryption of a digital video signal which is communicated from a computer system to an associated peripheral device, where the associated peripheral device decrypts the communicated digital video signal for use, the interface device comprising:

a digital video output;

digital video output formatting circuitry associated with said output;

a non-volatile RAM for containing a BIOS for controlling digital video output formatting having a specific write-protectable area allocated for storing an encryption key flag at a flag address and encryption key data;

said specific write-protectable area being rendered read-only when a predetermined flag value is stored at said flag address whereby encryption key data may be stored in said specific area of said non-volatile RAM in connection with storing said predetermined flag value at said flag address such that stored encryption key data cannot be altered by a subsequent write operation to said non-volatile RAM; and

said digital video interface device configured to receive as said predetermined value any value other than a specific value which specific value enables writing into said write-protectable area.

17. (Previously Presented) A digital video interface device according to claim 13 wherein said key flag is a combination of one or more values stored at the one or more flag addresses within said write-protectable area.

18. (Previously Presented) A digital video interface device according to claim 13 wherein the associated peripheral device is a digital display.

19. (Previously Presented) A digital video interface device according to claim 13 which is configured as a digital video interface card.

20. (Previously Presented) A digital video interface device according to claim 13 wherein said specific write-protectable area is at least 512k bytes and located at an address range higher than an address range reserved for a BIOS.

21. (Previously Presented) A method for producing digital video interface devices comprising:

providing a digital interface device having a digital output, digital video formatting circuitry associated with said output, and a non-volatile RAM for containing a BIOS for controlling digital video output formatting;

allocating a specific addressable area on said non-volatile RAM for storing an encryption key flag and encryption key data; and

rendering said specific area read-only only when a predetermined key flag value is written in said specific addressable area at a key flag address.

22. (Currently Amended) A method according to claim 21 further comprising:

writing a first predetermined flag value at said key flag address along with key encryption key data in said specific area to enable key encryption.

23. (Currently Amended) A method according to claim 21 further comprising:

writing a first predetermined flag value at said key flag address along with key encryption key data in said specific area to enable key encryption; or

writing a second predetermined flag value at said key flag address to permanently disable key encryption using said specific area.

24. (Previously Presented) A method according to claim 21 further comprising storing a specific value in said key flag address at the time the specific addressable area is allocated wherein said predetermined key value is any value other than said specific value.

25.(Currently Amended) A digital device for facilitating key encryption of a digital signal which is communicated to an associated device, where the associated device decrypts the communicated digital signal for use, the digital device comprising:

a digital output;

digital output formatting circuitry associated with said output;

a non-volatile RAM configured to control digital output formatting having a specific write-protectable area allocated;

said specific write-protectable area configured to store an encryption key flag at a flag address and encryption key data; and

said specific write-protectable area configured to be rendered read-only only when a predetermined flag value is stored at said flag address whereby encryption key data may be stored in said specific area of said non-volatile RAM in connection with storing said predetermined flag value at said flag address such that stored encryption key data cannot be altered by a subsequent write operation to said non-volatile RAM.

26. (Currently Amended) A digital device according to claim 25 configured to receive a first predetermined flag value at said flag address in association with key encryption key data in said specific write-protectable area which first flag value indicates encryption enablement.

27. (Currently Amended) A digital interface device according to claim 25 configured to receive either a first predetermined flag value at said flag address in association with key encryption key data in said specific write-

protectable area which first flag value indicates encryption enablement or a second predetermined flag value at said flag address which second flag value indicates encryption disablement in which case the digital interface device is permanently disabled from using the key encryption.

28. (Previously Presented) A method for producing digital devices comprising:

providing a digital device having a digital output, digital output formatting circuitry associated with said output, and a non-volatile RAM configured to control digital output formatting;

allocating a specific addressable area on said non-volatile RAM configured to store an encryption key flag and encryption key data; and

rendering said specific area read-only only when a predetermined key flag value is written in said specific addressable area at a key flag address.

29. (Currently Amended) A method according to claim 28 further comprising:

writing a first predetermined flag value at said key flag address along with ~~key~~ encryption <u>key</u> data in said specific area to enable key encryption.

30. (Currently Amended) A method according to claim 28 further comprising:

writing a first predetermined flag value at said key flag address along with ~~key~~ encryption <u>key</u> data in said specific area to enable key encryption; or

writing a second predetermined flag value at said key flag address to permanently disable key encryption using said specific area.